DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Cuadernos DivalData

Cuadernos dirigidos a delegados,
responsables y especialistas en protección
de datos personales

Cuaderno nº 33 | Marzo 2023

GESTIÓN DE PROVEEDORES EN EL SECTOR PÚBLICO: DEBER DE DILIGENCIA IN VIGILANDO

Í N D I C E

GESTIÓN DE PROVEEDORES EN EL SECTOR PÚBLICO: DEBER DE DILIGENCIA IN VIGILANDO

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirte a nuestra publicación accede al siguiente

enlace

"RGPD establece una obligación de diligencia debida en la elección de los encargados de tratamiento que deben aplicar todos los responsables, contratando únicamente encargados que estén en condiciones cumplir con el RGPD"

INTRODUCCIÓN

El art. 24. 1. Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (de ahora en adelante, RGPD) exige que el responsable aplique medidas técnicas y organizativas apropiadas y que las revise y actualice cuando sea necesario, a su vez en el art. 28.1 le indica al responsable que elegirá un proveedor/encargado que pueda aplicar medidas técnicas y organizativas suficientes.

El Considerando 81 RGPD resulta sumamente esclarecedor al señalar que el responsable (…) debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento (…).

Por eso, la Diputación de Valencia, de acuerdo con lo previsto en el art. 28 RGPD, va a ser responsable de que su proveedor/encargado del tratamiento (en los tratamientos que por cuenta del responsable realice) cumpla con el RGPD. En este sentido, Las "Directrices para la elaboración de contratos entre responsables y encargados de tratamiento" elaboradas por la Agencia Española de Protección de Datos (de ahora en adelante AEPD) la Agencia Vasca de Proteccion de Datos (de ahora en adelante, AVPD) y la Agencia Catalana de Proteccion de Datos (de ahora en adelante APDCAT)señalan que, el RGPD establece una obligación de diligencia debida en la elección de los encargados de tratamiento que deben aplicar todos los responsables, contratando únicamente encargados que estén en condiciones cumplir con el RGPD. Y ello, implica la necesidad de valorar si los encargados con los que se hayan contratado o se vayan a contratar operaciones de tratamiento, ofrecen garantías de cumplimiento del RGPD.

DILIGENCIA EN LA SELECCIÓN DE PROVEEDORES

La actuación diligente a la hora de elegir proveedor/encargado de tratamiento, no debe ser solo tarea de la Diputación, sino por extensión de sus propios encargados o subencargados; deben demostrar y acreditar que efectivamente cumplen con la normativa aplicable.

En este sentido, a fin de poder demostrar cumplimiento, el propio RGPD nos da algunas pautas o indicaciones, de lo que en determinados ámbitos resulta obligatorio tanto para responsables como para encargados, a saber:

a) Adopción e implantación de determinadas medidas como: seudonimización, minimización/reducción de tratamientos, transparencia, supervisión de tratamientos, promoción de desarrollo y fabricación de productos con una privacidad por defecto, etc. (C. 78 RGPD).

b) Revisión y actualización de medidas o controles que garanticen la seguridad del tratamiento (C.81 y art. 24.1 RGPD), previamente determinados y/o exigido al proveedor

c) Contar con un Registro de actividades de tratamiento (C. 82)

d) Adoptar las garantías adecuadas en los casos de estar ante una transferencia internacional de datos (decisión de la comisión, cláusulas contractuales tipo, etc. (C.108)

Sin ánimo de exhaustividad, el incumplimiento de la obligación de diligencia debida y, por tanto, la ausencia de control en materia de privacidad en la elección de un proveedor podría dar lugar a diferentes tipos de responsabilidad.

Los responsables asumen el nivel más alto nivel de responsabilidad: deben cumplir y demostrar el cumplimiento del RGPD y también son responsables del cumplimiento de su proveedor/encargado. De acuerdo con el art. 4.7) RGPD el responsable es “la

“A fin de poder demostrar cumplimiento, el propio RGPD nos da algunas pautas o indicaciones, de lo que en determinados ámbitos resulta obligatorio tanto para responsables como para encargados, a saber:

a) Adopción e implantación de determinadas medidas como: seudonimización, minimización/reducción de tratamientos, transparencia, supervisión de tratamientos, promoción de desarrollo y fabricación de productos con una privacidad por defecto, etc. (C. 78 RGPD).”

persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

ANÁLISIS DE LAS DISPOSICIONES

Como mencionábamos anteriormente del considerando 81 del Reglamento, se desprenden dos cuestiones a tener en consideración; por un lado, que los responsables del tratamiento deben ser diligentes a la hora de elegir a sus encargados y; por otro, que los encargados del tratamiento, con carácter previo a su contratación, tienen que ofrecer a los responsables las garantías que resulten adecuadas al nivel de riesgo identificado, facilitando las evidencias que permitan acreditar el cumplimiento de estas.

"la adhesión del encargado a un código de conducta o a un mecanismo de certificación aprobados por las autoridades de control competentes puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable".

En cuanto a lo anterior, el considerando del Reglamento, establece que la adhesión del encargado a un código de conducta o a un mecanismo de certificación aprobados por las autoridades de control competentes puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable.

En la actualidad, ni las autoridades de control competentes ni el Comité Europeo de Protección de Datos, han desarrollado los esquemas de certificación o aprobados suficientes códigos de conducta, para que las garantías enunciadas puedan ser aplicadas o tenidas en consideración por los responsables a la hora de seleccionar a sus encargados.

Entre los mecanismos que los responsables pueden implementar en sus organizaciones o los responsables podrán optar, bien por desarrollar e implementar políticas y procesos internos que les permitan llevar a cabo la evaluación y selección de proveedores de manera objetiva y evidenciable, o bien, contratar los servicios de un tercero de confianza que haya desarrollado unos criterios de evaluación propios.

En cuanto a la primera opción, es necesario que las políticas y procedimientos internos sean conocidas por todas las personas que participen en el proceso de selección, incluidas las unidades contratantes, siendo

imprescindible la formación y concienciación continua de dichas personas sobre la materia.

En este sentido, resulta recomendable que los criterios establecidos por el responsable para la selección de encargados del tratamiento, por ejemplo, en el momento de publicar una licitación, sean conocidos con carácter previo por éstos, de cara a que los tengan en cuenta a la hora de realizar sus ofertas a los responsables o participar en las licitaciones publicadas por aquellos.

¿QUÉ DEBEMOS TENER EN CUENTA?

El proceso de homologación de las garantías de estos proveedores, deberá ser transversal a todas las unidades implicadas en la selección de proveedores, pero además debe tener la capacidad o entidad suficiente para determinar si finalmente procede o no, iniciar la contratación del mismo.

Es importante conocer el escenario ante el que nos encontramos de cara a la identificación y clasificación de futuros proveedores, de manera que esto nos ayude a llevar a cabo una posterior evaluación exhaustiva y eficiente.

Lo siguiente pasos, a tener en cuenta cronológicamente, nos ayudaran a obtener el resultado deseado:

1. Identificación de todos los proveedores que vayan a tratar datos personales por cuenta de nuestra organización:

2. Análisis respecto a la tipología de los datos que van a ser tratados.

3. Análisis de la situación contractual.

4. Preparación de la evaluación y requisitos de cumplimiento normativo.

"Es importante conocer el escenario ante el que nos encontramos de cara a la identificación y clasificación de futuros proveedores, de manera que esto nos ayude a llevar a cabo una posterior evaluación exhaustiva y eficiente".

"El proceso de homologación ha de incluir la evaluación de la organización y gobernanza de la privacidad del proveedor, verificando y revisando la existencia de criterios relativos a protección de datos y otros aspectos del gobierno y cumplimiento de la normativa".

El proceso de homologación ha de incluir la evaluación de la organización y gobernanza de la privacidad del proveedor, verificando y revisando la existencia de criterios relativos a protección de datos y otros aspectos del gobierno y cumplimiento de la normativa como, por ejemplo:

- La posible adhesión a códigos de conducta.
- La posesión de un certificado de protección de datos.
- En su caso, el nombramiento de DPO y su registro ante la autoridad de control competente.
- La realización o no de Transferencias Internacionales de Datos, y en tal caso la existencia de garantías adecuadas para llevarla a cabo de acuerdo con la regulación.
- La llevanza de un Registro de Actividades de Tratamiento.
- La implementación de políticas internas relativas al tratamiento de datos personales (ejercicios de derechos, comunicación de incidentes de seguridad, gestión de personal etc.).
- La existencia de posibles subcontrataciones (subencargados del tratamiento y los correspondientes acuerdos de protección de datos con terceros).
- La existencia de antiguas sanciones al encargado del tratamiento en materia de protección de datos.
- La existencia de sentencias condenatorias y/o procedimientos judiciales abiertos en materia de protección de datos respecto del encargado del tratamiento.

CONSIDERACION DEL ENS

Por otro lado, hay que tener en consideración que esta obligación de diligencia debida también es exigida, más allá de la normativa general RGPD y estándares de aplicación, para la Diputación, debe cumplir con la aplicación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (de ahora en adelante, ENS).

Vemos por tanto, que en cuanto a la gestión de terceras partes en relaciones mercantiles de prestación de servicios que implique acceso a datos personales o a información confidencial en general de una organización, la relación Responsable de la Información proveedor de servicios está incluida en muchos estándares y legislación que obliga a un control diligente por parte del Responsable y que incluye una serie de obligaciones de control y diligencia en las diferentes fases de la relación: pre, contractual y postcontractual, más allá del RGPD. En el caso del ENS se incluye entre sus requisitos mínimos la obligación de la AAPP de verificar que todo producto que adquiera o contrate cumpla con todos los requisitos del ENS, debiendo valorarse positivamente las certificaciones en cuanto a seguridad que aporte.

Además, las medidas de seguridad obligatorias para toda la información tratada un apartado de Servicios Externos.

Dado que cualquier proveedor de las AAPP españolas está obligado a cumplir con el ENS, incluir entre las obligaciones internas a cumplir las de diligencia y gestión de terceras partes, siguiendo las directrices del ENS, puede simplificar procesos internos y dar luz a tareas y medidas a implantar en el proceso de diligencia en la gestión de terceros.

Asi, se expone en el Anexo II, Medidas de Seguridad del ENS, más concretamente en las medidas del marco operacional referentes a los Servicios Externos, “Gestion Diaria” donde se establece que para la gestión diaria del sistema, se establecerán los siguientes puntos;

– Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio, incluyendo el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordada

“Dado que cualquier proveedor de las AAPP españolas está obligado a cumplir con el ENS, incluir entre las obligaciones internas a cumplir las de diligencia y gestión de terceras partes, siguiendo las directrices del ENS, puede simplificar procesos internos y dar luz a tareas y medidas a implantar en el proceso de diligencia en la gestión de terceros”.

– El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas comprendidos en el acuerdo, que contemplarán los supuestos de incidentes y desastres

Tener en cuenta que estos últimos puntos serán de aplicación siempre que estemos ante sistemas de categoría MEDIA, tal y como dispone la norma.

.

"Como justificación a la exclusión del consentimiento como base de licitud, alude a la posición de desequilibrio entre el ciudadano como interesado y la Administración como Responsable del tratamiento, lo que hace que no se pueda contar con un consentimiento válido al no basarse en una "manifestación de voluntad libre".

MATERIAL COMPLEMENTARIO

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, («RGPD») relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Consulta este enlace.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Consulta este enlace.
- Guía "Directrices para la elaboración de contratos entre responsables y encargados del tratamiento". Consulta este enlace.
- Guía de Computing Cloud para entidades que contraten servicios. Consulta este enlace.

NOTICIAS

- **La Comisión Europea prohíbe a su personal usar TikTok "para proteger sus datos y aumentar su ciberseguridad"**

  El Parlamento Europeo ha acabado por sumarse a las otras dos grandes instituciones europeas y ha vetado el uso de TikTok en sus dispositivos a eurodiputados y empleados. La Comisión Europea y el Consejo de la UE adoptaron esta decisión la semana pasada para sus funcionarios y cinco días después les ha seguido la Eurocámara. La aplicación china se ha convertido en los últimos tiempos en fuente de sospechas en Occidente por "la protección de datos y la recogida de datos para terceras partes", según puede leerse en el mensaje que han recibido los parlamentarios.

  A la lista de Gobiernos que vetan el uso de este programa informático en los dispositivos electrónicos utilizados por sus empleados se sumó este lunes Canadá: "La decisión de eliminar y bloquear TikTok de los dispositivos móviles de las administraciones públicas se adopta por precaución, en particular por la inquietud que suscita el régimen jurídico que rige la información recopilada de los dispositivos, y está en consonancia con el planteamiento de nuestros socios internacionales. En un dispositivo móvil, los métodos de recopilación de datos de TikTok proporcionan un acceso considerable al contenido del teléfono", apunta el comunicado con el que se dio a conocer la decisión.". Consulta la noticia en este enlace.